

In the Claims

Claims 1, 7, 13, 18, 22, 26-31 are amended.

Claims 32-34 are canceled.

Claims 1-31 are pending and are listed as follows:

1. **(Currently Amended)** A Web server input string screening method comprising:

determining an attack pattern that can be used to attack a Web server, the attack pattern comprising content that ~~is designed to constitute~~ is determined as constituting one or more of a disclosure attack or ~~or~~ [[,]] an integrity attack ~~or a denial-of-service attack~~ on the Web server;

defining a search pattern that can be used to detect the attack pattern, the search pattern being defined in a manner that permits variability among its constituent parts;

receiving an input string that is intended for use by a Web server;

evaluating the input string using the search pattern to ascertain whether the attack pattern is present; and

implementing a remedial action if an attack pattern is found that matches the search pattern.

2. **(ORIGINAL)** The Web server input string screening method of claim 1, wherein:

said defining comprises defining a plurality of different search patterns; and

said evaluating comprises evaluating the input string using said plurality of different search patterns.

1
2 3. (ORIGINAL) The Web server input string screening method of
3 claim 1, wherein the search pattern is specified as a regular expression.
4

5 4. (ORIGINAL) The Web server input string screening method of
6 claim 1, wherein said receiving of the input string comprises receiving a URL.
7

8 5. (ORIGINAL) The Web server input string screening method of
9 claim 1, wherein said receiving of the input string comprises receiving a portion of
10 an HTTP verb request.
11

12 6. (ORIGINAL) The Web server input string screening method of
13 claim 1, wherein said implementing comprises denying a request that is associated
14 with the input string.
15

16 7. (Currently Amended) A Web server input string screening method
17 comprising:

18 defining one or more search patterns that comprise literal characters and
19 special characters, wherein the literal characters indicate exact characters in an
20 input string that is intended for receipt by a Web server, and the special characters
21 indicate variable characters in an input string that is intended for receipt by the
22 Web server, the search patterns being usable to search for an attack pattern that
23 can be used to attack the Web server, the attack pattern comprising content that is
24 ~~designed to constitute~~ determined as constituting one or more of a disclosure
25

1 attack or ~~[[,]]~~ an integrity attack ~~or a denial of service attack~~ on the Web server;
2 and

3 storing the one or more search patterns in a memory location that is
4 accessible to a screening tool for evaluating an input string that is intended for
5 receipt by the Web server.

6
7 8. (ORIGINAL) The Web server input string screening method of
8 claim 7 further comprising:

9 retrieving a search pattern from the memory location; and
10 evaluating an input string with the screening tool by ascertaining whether
11 the input string includes at least a portion that matches the search pattern.

12
13 9. (ORIGINAL) The Web server input string screening method of
14 claim 8, wherein the evaluating of the input string comprises evaluating a URL.

15
16 10. (ORIGINAL) The Web server input string screening method of
17 claim 8, wherein the evaluating of the input string comprises evaluating a portion
18 of an HTTP verb request.

19
20 11. (ORIGINAL) The Web server input string screening method of
21 claim 7 further comprising implementing the screening tool as an extension for an
22 existing Web server.

23
24 12. (ORIGINAL) The Web server input string screening method of
25 claim 7 further comprising implementing the screening tool as an ISAPI extension.

1
2 13. (Currently Amended) A Web server input string screening method
3 comprising:

4 defining one or more search patterns that are specified as a regular
5 expression, the search patterns being usable to search for an attack pattern that can
6 be used to attack the Web server, the attack pattern comprising content that is
7 ~~designed to constitute~~ determined as constituting one or more of a disclosure
8 attack or ~~or~~ [[,]] an integrity attack ~~or a denial-of-service attack~~ on the Web server,
9 and

10 storing the one or more search patterns in a memory location that is
11 accessible to a screening tool for evaluating an input string that is intended for
12 receipt by the Web server.
13

14 14. (ORIGINAL) The Web server input string screening method of
15 claim 13 further comprising:

16 retrieving a search pattern from the memory location; and
17 evaluating an input string with the screening tool by ascertaining whether
18 the input string includes at least a portion that matches the search pattern.
19

20 15. (ORIGINAL) The Web server input string screening method of
21 claim 14, wherein the evaluating of the input string comprises evaluating a URL.
22

23 16. (ORIGINAL) The Web server input string screening method of
24 claim 14, wherein the evaluating of the input string comprises evaluating a portion
25 of an HTTP verb request.

1
2 17. (ORIGINAL) A computer-readable medium having computer-
3 readable instructions thereon which, when executed by a computer, perform the
4 method of claim 14.

5
6 18. (Currently Amended) A Web server input string screening tool
7 embodied on a computer-readable medium comprising:

8 a pattern matching engine that is configured to receive an input string that
9 is intended for use by a Web server and evaluate the input string to ascertain
10 whether it likely constitutes an attack on the Web server, the attack comprising
11 one or more of a disclosure attack or ~~or~~ [[,]] an integrity attack ~~or a denial of service~~
12 ~~attack~~ on the Web server; and

13 one or more patterns that are usable by the pattern matching engine to
14 evaluate the input string, the patterns being defined in a manner that permits
15 variability among the constituent parts of the one or more patterns.

16
17 19. (ORIGINAL) The Web server input string screening tool of claim
18 18, wherein the one or more patterns are specified as regular expressions.

19
20 20. (ORIGINAL) The Web server input string screening tool of claim
21 18, wherein the pattern matching engine is configured to receive an input string
22 that comprises a URL.

1 21. **(ORIGINAL)** The Web server input string screening tool of claim
2 18, wherein the pattern matching engine is configured to receive an input string
3 that comprises a portion of an HTTP verb request.

4
5 22. **(Currently Amended)** One or more computer readable media
6 having computer-readable instructions thereon which, when executed by a
7 computer perform the following steps:

8 receiving an input string that is intended for use by a Web server;
9 evaluating the input string using a search pattern to ascertain whether the
10 input string contains an attack pattern that can be used to attack the Web server,
11 the attack pattern comprising content that is ~~designed to constitute~~ determined as
12 constituting one or more of a disclosure attack or ~~or~~ [[,]] an integrity attack ~~or a~~
13 ~~denial of service attack~~ on the Web server, the search pattern comprising literal
14 characters and special characters, wherein literal characters indicate exact
15 characters in the input string, and the special characters indicate variable
16 characters in the input string; and

17 implementing a remedial action if an attack pattern is found that matches
18 the search pattern.

19
20 23. **(ORIGINAL)** The computer-readable media of claim 22, wherein
21 said implementing comprises denying a request that is associated with the input
22 string.

1 24. (ORIGINAL) The computer-readable media of claim 22, wherein
2 said receiving comprises receiving a URL.

3
4 25. (ORIGINAL) The computer-readable media of claim 22, wherein
5 said receiving comprises receiving an input string that is associated with an HTTP
6 verb request.

7
8 26. (Currently Amended) A ~~collection of Web server screening~~
9 ~~patterns embodied on a computer readable medium~~ Web server comprising:

10 a processor and one or more computer-readable media;

11 ~~a memory; and~~

12 a plurality of patterns stored in the ~~memory~~ one or more computer-readable
13 media, the patterns being useable by the Web server processor to screen input
14 strings ~~that are intended for use by a Web server~~ to ascertain whether the input
15 strings comprise attack patterns, the attack patterns comprising content that is
16 ~~designed to constitute~~ determined as constituting one or more of a disclosure
17 attack or ~~or~~ [[.]] an integrity attack ~~or a denial of service attack~~ on the Web server,
18 individual patterns being defined in a manner that permits variability among their
19 constituent parts.

20
21 27. (Currently Amended) The ~~collection system~~ collection system of claim 26, wherein
22 the patterns are specified as regular expressions.

23
24 28. (Currently Amended) The ~~collection system~~ collection system of claim 26, wherein
25 the collection is adapted for addition to, deletion of, or modification of patterns.

1
2 29. (Currently Amended) The ~~collection~~ system of claim 26, wherein
3 the patterns are configured for use in screening URLs that are intended for use by
4 a Web server.

5
6 30. (Currently Amended) The ~~collection~~ system of claim 26, wherein
7 the patterns are configured for use in screening input strings associated with HTTP
8 verb requests that are intended for use by a Web server.

9
10 31. (Currently Amended) The ~~collection~~ system of claim 26
11 configured for use by an ISAPI extension.

12
13 32.-34. (Canceled).
14
15
16
17
18
19
20
21
22
23
24
25